THE HONORABLE ROBERT S. LASNIK

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	No. CR19-159-RSL **DEFENDANT'S ADDENDUM TO THE SUBSTANTIVE PRETRIAL MOTIONS**

I. INTRODUCTION

After the defense filed three substantive pretrial motions in this case, (1) a motion to dismiss Counts 1, 9, and 10; (2) a motion to dismiss Counts 2-8 (the CFAA counts); and (3) a motion to strike the crypto mining allegations of Count 1 and to sever Count 8, (Dkt. Nos. 122-124), the government—no doubt recognizing infirmities in its charging document—filed a second superseding indictment on January 12, 2022. (Dkt. No. 166.) At a status conference on February 11, 2022, the Court invited the defense to submit an addendum to its motions in light of the second superseding indictment before it holds oral argument on March 15, 2022.

The defense submits this addendum to provide the Court with additional legal authority for its consideration of the motion to dismiss Counts 2-8 with prejudice. The Court will hear oral argument for that motion on March 15, 2022.

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

The defense also asks the Court to reconsider part of its ruling on February 28, 2022, and submits this addendum in support of its request for reconsideration of the motion to dismiss Counts 1, 9, and 10. At the time the Court issued its written opinion regarding that motion, which denied dismissal but granted, in part, a bill of particulars, (Dkt. No. 202), the defense was working on this addendum. The defense believes that the issues discussed in this addendum are essential to the Court's consideration of that motion. Thus, the defense asks the Court to reconsider its ruling on that motion alongside this addendum.

The defense submits no additional argument based in connection with the motion to strike and sever. The Court will hear argument on that motion on March 15 as well, and the defense will address that motion at that time.

***

Because the second superseding indictment does not correct in any meaningful way the legal deficiencies in the indictment or first superseding indictment, the parties agree that the existing briefing on these issues do not need to be re-filed, and the Court can rule on the motions as they apply to the second superseding indictment.[1]

II. ARGUMENT

The second superseding indictment did not cure the defects identified in the defense's three motions. Additionally, the Second Circuit and the United States Supreme Court issued material rulings after the defense filed its motions and after the grand jury returned the second superseding indictment. Those rulings further undermine the government's positions with respect to the defense's motions to dismiss Counts 1, 9, and 10 and Counts 2-8.

//

[1] The defense's various motions to compel are also unaffected by the filling of the second superseding indictment and should be granted. (*See* Dkt. Nos. 111, 127, 149.)

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

a. Motion to Dismiss Counts 1, 9, and 10 (Dkt. No. 122)

The government's addition of the term "roles" to multiple parts of the second superseding indictment is its most substantive amendment, (Dkt. No. 166, ¶¶ 11, 13, 14, 15, 16, 21, 22) and represents a significant "clarif[ication.]" (Dkt. No. 138 at 8.) This clarification, however, further supports the defense's motion to dismiss Counts 1, 9, and 10 because a "role" is not a password or access key—it is a signifier that the underlying server uses *to provide concomitant security credentials* for your session. (Dkt. No. 138 at 3, fn. 1.) To give a less nebulous example, IT administrators often set up certain "roles" within a company such as "administrator" and "user" to differentiate the ability to access certain resources on the network. If the computer system recognizes the person logging on as an "administrator," it will provide that person with underlying access to certain network resources that a "user" could not access.

In Ms. Thompson's case, the second superseding indictment essentially alleges that she showed up at an open door and the IT administrators, due to a misconfiguration of their own making, gave her an "administrator" role. In finding that Ms. Thompson's actions could arguably constitute wire fraud, the Court relied on the 2019 Northern District of Illinois case *United States v. Vorely*, which held that an "implied misrepresentation" could constitute wire fraud in the context of "spoofed" commodities orders. (Dkt No. 202 at 6-7 *citing* 420 F. Supp. 3d 784 (N.D. Ill. 2019).) But the reasoning in *Vorely* was severely undercut by the Second Circuit in *United States v. Connolly*, which was decided on January 27, 2022. 24 F.4th 821 (2d Cir. 2022). The Court should rely on the reasoning of *Connolly*, not *Vorely*, in resolving the motion to dismiss Counts 1, 9, and 10.

In *Connolly*, the Second Circuit held that statements made by the defendants to putatively affect the London Interbank Offered Rate ("LIBOR") were not false or deceptive within the meaning of the wire fraud statute. *Id.* at 832-33. In so holding, the

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

Second Circuit found that even if the representations were made wrongfully or with bad intent, "[i]f the rate submitted is one that the bank could request, be offered, and accept, the submission, irrespective of its motivation, would not be false." *Id.* at 835. Thus, the Second Circuit found that an implied misrepresentation is not enough to constitute wire fraud because the government is *always* bound to prove a material falsehood, half-truth, or fraudulent omission. *See id.* at 834. Although a scheme to defraud "need not succeed in order to violate § 1343 . . . to come within the scope of § 1343 it must at least be a scheme to defraud." *Id.* at 839.

Here, the government claims that Ms. Thompson made false representations to gain security credentials to access the alleged victims' servers. (Dkt No. 166 at ¶ 11.) But that is inaccurate; Ms. Thompson accessed a public IP address through a port that was open (whether purposefully or inadvertently) and made no misrepresentations – implied or otherwise. The computer system provided her "administrator" privileges—she did not steal them or make a "misrepresentation" to any computer system to gain them—at most, she executed publicly known commands to which the AWS-designed systems were designed to respond to *for anybody*. The second superseding indictment provides no demonstrable theory as to how accessing a public computer and executing publicly known commands on that computer constitutes a legally cognizable "scheme to defraud." Instead, the government attempts to obfuscate how these alleged credentials were "stolen" by stating that Ms. Thompson "transmitted commands to the misconfigured servers that obtained the security credentials for particular accounts and roles." (*Id.* at ¶ 13.) But the government wholly fails to demonstrate how any transmission of publicly available and rather innocuous commands were "false" within the meaning of the wire fraud statute.

The government may not like Ms. Thompson's alleged behavior, but the "federal fraud statutes are not catch-all laws designed to punish all acts of wrongdoing or

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

dishonorable practices." *Connolly*, 24 F. 4th at 834. To subject Ms. Thompson to the vagaries of trial under a theory that should, as a matter of law, result in an acquittal pursuant to Federal Rule of Criminal Procedure 29 in the hopes that the jury will convict Ms. Thompson on the basis of confusion or other irrelevant and inflammatory evidence (such as the cryptojacking allegations made here) is improper. *See United States v. White*, 766 F. Supp. 873 (E.D. Wash. 1991) (finding that it was proper to dismiss charges under a novel and legally unsupportable *mens rea* theory after a bill of particulars because it was not proper to "forc[e] someone to undergo a trial for no purpose"); *cf. United States v. King*, 259 F. Supp. 3d 1267, 1285 (W.D. Okla. 2014) (finding it appropriate to use a bill of particulars to establish venue when there was a "serious question" about lack of venue such that the "right not to be tried" be upheld).

Additionally, with regards to Count 9, the Court should reconsider its decision to dismiss (or order a bill of particulars) because the Ninth Circuit's recent decision in *United States v. Saini*, 23 F.4th 1155, 1160-61 (9th Cir. 2022) made clear that "intent to defraud" under the access device fraud statute, 18 U.S.C. § 1029, requires the "intent to deceive *and* cheat." The second superseding indictment fails to properly allege the requisite *mens rea* in a way that complies with the *Saini* ruling.

For all these reasons, the Court should reconsider its decision as to the motion to dismiss Counts 1, 9, and 10 and dismiss those counts with prejudice. To the extent that it does not do so, the Court should, at least, order an additional bill of particulars as to them such that Ms. Thompson is informed as to exactly *which* credentials the government believes were "false" and on what basis.

b. <u>Motion to Dismiss Counts 2-8 (Dkt. No. 123)</u>

As explained above, the second superseding indictment makes clear that Ms. Thompson did not steal or hack a long-term security credential, such as a password or access key, but rather, at most, assumed a "role" that the AWS servers automatically

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

assigned to her once she accessed the public port. This clarification makes the government's analogy in its opposition to Ms. Thompson's motion to dismiss Counts 2-8, that "[s]canning for misconfigured ports is a bit like walking down the street, testing handles to see which doors have been left unlocked by mistake," even more inapt. (Dkt. No. 135 at 4.)

To use the government's analogy, walking down the street and testing door handles to see which houses are open does not automatically assign you the role of "homeowner," but that is what the AWS servers did here for anybody. Ms. Thompson's purported access was not unauthorized because the "gate" established by the alleged victim entities was left open to the public and, in such an instance, the alleged victims' WAFs permitted her (or anyone else who accessed the public port in the same way) such access. *See Domain Name Comm'n Ltd. v. DomainTools LLC*, 449 F. Supp. 3d 1024, 1027 (W.D. Wash. 2020) (Lasnik, J.) (stating that whether access is authorized depends on the actions taken by the owner of the computer system). Information about how to prevent a WAF from permitting such access was freely and publicly. The alleged victim entities simply *chose* not to program their WAFs to eliminate public access. That choice should result in the dismissal of Counts 2-8.

Further, the Supreme Court's very recent decision in *Wooden v. United States*, ___ S. Ct. ___, No. 20-5279, 2022 WL 660610 (Mar. 7, 2022) further supports the dismissal of those charges because it underscores that the rule of lenity bars her prosecution under the Computer Fraud and Abuse Act ("CFAA"). This is because the CFAA did not give her fair notice that the behavior described by the government would constitute *unauthorized* computer access and because she could not have formed the requisite *mens rea* for such crime.

In *Wooden*, the Supreme Court issued a plurality decision as to the meaning of the Armed Career Criminal Act's ("ACCA's) "occasions" clause. *Id.* In concurring

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

opinions, Justices Sotomayor, Gorsuch, and Kavanaugh found that the rule of lenity further supported the Court's decision to limit the prosecution's attempt to expand the ACCA. *Id.* at *8 (Sotomayor, J., concurring); *9-10 (Kavanaugh, J., concurring); and *13-19 (Gorsuch, J., concurring). In their opinion, Justices Gorsuch and Sotomayor made clear that the rule of lenity "works to enforce the fair notice requirement by ensuing that an individual's liberty always prevails over ambiguous laws." *Id.* at *15 (Gorsuch, J. and Sotomayor, J., concurring). Although lenity "carries its costs" and "some cases will fall through the gaps," lenity protects "an indispensable part of the rule of law—the promise that, whether or not individuals happen to read the law, they can suffer penalties only for violating standing rules announced in advance." *Id.* at *16 (Gorsuch, J. and Sotomayor, J., concurring). Justice Kavanaugh also recognized the "importance of fair notice in federal criminal law," but focused instead on the concept of *mens rea* as opposed to the ambiguity of statutory construction. *Id.* at *10 (Kavanaugh, J., concurring).

As made clear in the defense's motion to dismiss Counts 2-8, the text of the CFAA and courts' interpretation of it to date failed to give Ms. Thompson "fair notice" that accessing a WAF through a publicly available port could constitute the federal crime of *unauthorized* computer access. Beyond that, "vigorous" application of the *mens rea* requirements, as advocated by Justice Kavanaugh, also lays bare that unless the government is intending to prosecute every white hat hacker in the United States, scanning public ports for misconfigurations and then being automatically granted "administrator" access by a misconfigured server is not *unauthorized* access of a computer system as required by the CFAA.

Indeed, for all the reasons cited above and in the defense's motion to dismiss Counts 1, 9, and 10, nothing in the text of the wire fraud, access device fraud, or aggravated identity theft statues gave Ms. Thompson fair notice that her alleged

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

behavior would have violated those statutes, either. And, as argued above, the government has failed to allege the requisite *mens rea* because there was no false statement made nor any intent made to both deceive *and* cheat. *Wooden* thus supports dismissal of the entire second superseding indictment.

III. CONCLUSION

For all of the above-stated reasons, as well as all of the reasons stated in the defense's filings to date, the Court should grant the defense's three substantive pretrial motions.

DATED: March 11, 2022

Respectfully submitted,

/s/ *Mohammad Ali Hamoudi*
MOHAMMAD ALI HAMOUDI
/s/ *Christopher Sanders*
CHRISTOPHER SANDERS
/s/ *Nancy Tenney*
NANCY TENNEY
Assistant Federal Public Defenders

/s/ *Brian Klein*
BRIAN KLEIN
/s/ *Melissa Meister*
MELISSA MEISTER
Waymaker LLP

Attorneys for Paige Thompson

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100